REMARKS

Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1, 3-9, 11-22 and 46-54 are currently pending.
- Claims 1, 46, 48 and 52 are amended herein.
- No claims are canceled herein.
- No claims are withdrawn herein.
- No new claims are added herein.

Claim Objections

Claim 8 stands objected to as allegedly not being clear as to its status as an independent or independent claim. For convenience to the reader, claim 8 is provided below:

> **8. (Original)** A computing device comprising:
> an input device for receiving one or more input streams;
> a medium as recited in claim 1.

According to 37 CFR § 1.75(c), a dependent claim is one that "refer[s] back to and further limit[s] another claim or claims in the same application." The language of claim 8 indicates that its medium is the one "recited in claim 1." This claim language refers back to claim 1. Also, claim 8 further limits claim 1 by including the medium of claim 1 as part of a computing device. Accordingly, Applicant asks for the withdrawal of the objection to claim 8.

Claims 1, 3-7, 46, 49 and 52 Recite Statutory Subject Matter Under § 101

Claims 1, 3-7, 46, 49 and 52 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicant respectfully traverses this rejection.

On p. 2 of the Action, the Office indicates the following:

> 7. Claims 1, 3-7, 46, 49 and 52 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1, 3-7, 46, 49 and 52 recite "a computer-readable storage medium" wherein the computer-readable storage medium is not explicitly defined to be limited to the statutory subject matter. Therefore, claims 1, 3-7, 46, 49 and 52 read in light of the specification includes a non-statutory subject matter.

According to the specification (¶ [0136] of the U.S. Patent Application Publication No. 20050084101), a "computer storage medium" is described in this manner:

> "Computer storage media" include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by a computer.

This description appears to include only statutory subject matter. Perhaps, the Office is confused by the inclusion of the word "readable" in the claims after the word "computer." If so, Applicant amends the rejected independent claims to remove the word "readable" so that the text matches precisely the term used in the specification.

Nevertheless, for the sole purpose of expediting prosecution and without commenting on the propriety of the Office's rejections, Applicant herein amends claims 1, 46, 49 and 52 as shown above. Applicant respectfully submits that these amendments render the § 101 rejection moot.

Expectation that the Next Action will not be Final

Applicant submits that all pending claims are in condition for allowance. If the examiner feels otherwise and believes that another action on the merits is necessary, then Applicant expects such an action would be Non-Final.

According to 37 CFR § 1.113 and MPEP § 706.07, the "examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal." "The invention as disclosed and claimed should be thoroughly searched in the first action and the references fully applied."

In accordance with 37 CFR § 1.113 and MPEP § 706.07(a), Applicant respectfully submits that finality would be premature for the next action because the Office, in this Action, fails to address specific claimed aspects that differ from the cited art and because the Applicant takes no action necessitating new grounds for rejection or a new search.

Herein, Applicant does not and has not amended any claim to overcome any cited art. Consequently, one or more claims presented herein have already been examined in the Office Action. Furthermore, Applicant explains herein why these already-examined claims differ from the cited art of record. Therefore, in accordance with 37 CFR § 1.113 and MPEP § 706.07(a), finality for the next action would be premature.

Rejecting claims without specific support or reasoning

In the rejection of claim 52 on p. 5 of the Action, the Office fails to address all of the claimed elements. In particular, the Office does not cite any references (alone or in combination) that disclose, teach or suggest this claimed element: "maintaining the intervening while the subject input stream is being played." Furthermore, the Office Action fails to provide any reason why one of ordinary skill in the art would combine the missing teaching with the teachings of the cited references.

Applicant's Right to Adequately Respond

Because the Office has not fully addressed all of the elements of all of the pending claims in its rejection of all of the claims, Applicant can do little more than gainsay when forming its reply. Applicant is forced to make assumptions and guesses as to the Office's specific reasoning. Therefore, Applicant submits that it has been denied its right to adequately and effectively respond to the Office's rejections.

In *In re Lee*, 61 USPQ2d 1430 (CA FC 2002), the Federal Circuit explained the following on page 1433:

> The Administrative Procedure Act, which governs the proceedings of administrative agencies [such as the Patent and Trademark Office] and related judicial review,

> establishes a scheme of "reasoned decisionmaking." Not only must an agency's decreed result be within the scope of its lawful authority, but the process by which it reaches that result must be logical and rational. Allentown Mack Sales and Service, Inc. v. National Labor Relations Bd., 522 U.S. 359, 374 (1998) (citation omitted).
>
> This standard requires that the agency not only have reached a sound decision, but have *articulated the reasons for that decision*. The reviewing court is thus enabled to perform meaningful review within the strictures of the APA, for the court will have a basis on which to determine "whether the decision was based on the relevant factors and whether there has been a clear error of judgment." Citizens to Preserve Overton Park v. Volpe, 401 U.S. 402, 416 (1971). [emphasis added]

Applicant submits that the Office has not articulated the reasons for its decision-making here. Furthermore, according to the reasons and facts given above and to 37 CFR § 1.113 and MPEP § 706.07, Applicant respectfully submits that no clear issues hav3 been developed between the Applicant and the Examiner for each pending claim so that such issues would be ready for appeal if the next action is made final. Accordingly, Applicant respectfully requests that the next action—if not a Notice of Allowance—be Non-Final.

Cited Documents

The following documents have been applied to reject one or more claims of the Application:

- **Lenoir:** Lenoir et al., U.S. Patent No. 6,671,806;
- **Cox**: Cox et al., "Some general methods for tampering with watermarks," IEEE, 1998, pp. 1-15; and

- **Tobias:** Tobias et al., WO01/24530.

Claims 1, 4-9, 12-18, 20-22 and 48-52 are Non-Obvious Over Lenoir in View of Cox

Claims 1, 4-9, 12-18, 20-22 and 48-52 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Lenoir in view of Cox. Applicant respectfully traverses the rejection.

Independent Claim 1

Claim 1 recites, in part:

> observing and determining a location in a processor-readable memory of a computer, where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform detection thereon to determine if the stream has an embedded-signal therein;
>
> intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector.

On p. 3 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "observing and determining" element and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject

input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

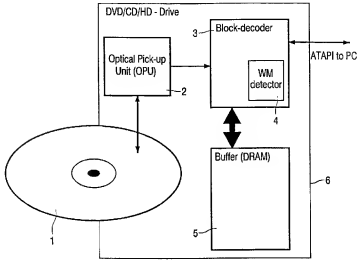

Figure 1 of Lenoir

As shown in Fig. 1 of Lenoir above and described in Lenoir at col. 4, lines 1-18, the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "observing and determining a location in a processor-readable memory...where [the watermark detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in Lenoir buffer

has not been received by the Lenoir's watermark detector. Therefore, Lenoir fails to teach "observing and determining a location in a processor-readable memory...where [the watermark detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (see Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "intervening with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Cox's "transformations" and "attacks" do not include the "intervening," as claimed. Instead, Cox describes pixel shifting, adding random noise of

a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 1.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 1. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 1.

Dependent Claims 4-8

Claims 4-8 ultimately depend from independent claim 1. As discussed above, claim 1 is allowable over the cited documents. Therefore, claims 4-8 are also allowable over the cited documents of record for at least their dependency from an allowable base claim, and also for the additional features that each recites.

Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claims 4-8.

Independent Claim 9

Claim 9 recites, in part:

> observing and determining a location in a processor-readable memory of a computer configured to receive a subject input stream for the watermark, the location being where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input

stream for the watermark to perform detection thereon to determine if the stream has an embedded-signal therein;

intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector.

On p. 3 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "observing and determining" element and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "observing and determining a location in a processor-readable memory…where [the watermark detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector

processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer is not been received by the Lenoir's watermark detector. Therefore, Lenoir fails to teach "observing and determining a location in a processor-readable memory...where [the watermark detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "intervening with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the

copy control mechanism. Cox's "transformations" and "attacks" do not include the "intervening," as claimed. Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 9.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 9. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 9.

Dependent Claims 12-16

Claims 12-16 ultimately depend from independent claim 9. As discussed above, claim 9 is allowable over the cited documents. Therefore, claims 12-16 are also allowable over the cited documents of record for at least their dependency from an allowable base claim, and also for the additional features that each recites.

Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claims 12-16.

Independent Claim 17

Claim 17 recites, in part:

> a memory-location determiner ("watermark-detector detector") configured to determine where a dynamic embedded-signal detection program module ("watermark

detector") receives a subject input stream for the watermark detector to perform detection thereon to determine if the stream has an embedded-signal therein;

an intervention component configured to intervene with clear reception of the subject input stream by the watermark detector, thereby hindering watermark detection by the watermark detector.

On p. 3 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "memory-location determiner" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervention component" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determin[ing] where [the watermark detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to

Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer has not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determin[ing] where [the watermark detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "interven[ing] with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the

copy control mechanism. Cox's "transformations" and "attacks" do not include the "intervening," as claimed. Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 17.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 17. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 17.

Dependent Claims 18 and 20-22

Claims 18 and 20-22 ultimately depend from independent claim 17. As discussed above, claim 17 is allowable over the cited documents. Therefore, claims 18 and 20-22 are also allowable over the cited documents of record for at least their dependency from an allowable base claim, and also for the additional features that each recites.

Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claims 18, and 20-22.

Independent Claim 48

Claim 48 recites, in part:

> a memory-location determiner ("watermark-detector detector") configured to determine where, in a memory, an

embedded-signal detection program module ("detector") receives a subject input stream for the detector to perform detection thereon to determine if the subject input stream has an embedded-signal therein and further configured to detect and observe the detector in a processor-readable memory of a computer to determine its location in such memory;

an intervention component configured to intervene with clear reception of the subject input stream, thereby hindering watermark detection by the detector, wherein the intervening comprises adjusting an incoming rate for the input stream.

On pp. 5-6 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "memory-location determiner" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervention component" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of a subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing

on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determin[ing] where, in a memory, [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer has not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determin[ing] where, in a memory, [the detector] receives a subject input stream."

Furthermore, Lenoir fails to teach "detect[ing] and observ[ing] the detector in a processor-readable memory of a computer to determine its location in such memory," as claimed. As noted above, Lenoir's watermark detector 4 is integrated with the block decoder 3. It is not part of the buffer 5, which Lenoir indicates might be vulnerable to hackers. (*See* col. 4, lines 11-13). The Office has not identified (with or without any particularity) where Lenoir or any reference teaches "detect[ing] and observ[ing] the detector in a processor-readable memory of a computer to determine its location in such memory," as claimed.

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "interven[ing] with clear reception of the subject input stream...hindering watermark detection by the detector... adjusting an incoming rate for the input stream."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. The "transformations" and "attacks", as listed and described by Cox, do not include adjusting the play-rate of the incoming stream. Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 48.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 48. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 48.

Independent Claim 49

Claim 49 recites, in part:

> determining where, in a memory, a dynamic watermark detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform watermark detection thereon to determine if the subject input stream has an embedded-signal therein;
>
> intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the intervening comprises introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal.

On pp. 6-7 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "determining" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically

collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (oCl. 4, lines 6-9).

This claim recites "determining where, in a memory, [the watermark detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer is not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determining where, in a memory, [the watermark detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes, "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "intervening with clear reception of the subject input stream...hindering watermark

detection by the detector...introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. The "transformations" and "attacks", as listed and described by Cox, do not include introducing a countersignal into the incoming stream. Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 49.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 49. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 49.

Independent Claim 50

Claim 50 recites, in part:

> determining a location in a processor-readable memory of a computer configured to dynamically detect an embedded-signal in an input stream, the location being where a dynamic embedded-signal detection program

module ("dynamic detector") receives a subject incoming stream for the dynamic detector to perform detection thereon to determine if the subject incoming stream has an embedded-signal therein;

intervening with clear reception of the subject incoming stream, thereby hindering detection by the dynamic detector, wherein the intervening comprises modifying the reception by introduction of a noise countersignal into the incoming stream.

On pp. 6-7 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "determining" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determining a location in a processor-readable memory...where [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer is not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determining a location in a processor-readable memory...where [the detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "intervening with clear reception of the subject input stream...hindering watermark detection by the detector...modifying the reception by introduction of a noise countersignal into the incoming stream."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. The "transformations" and "attacks", as listed and described by Cox, do not include "modifying the reception by introduction of a noise countersignal into the incoming stream." Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 50.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 50. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 50.

Independent Claim 51

Claim 51 recites, in part:

> a memory-location determiner ("watermark-detector detector") configured to determine a location where, in a memory, an embedded-signal detection program module ("detector") receives a subject incoming stream for the

detector to perform detection thereon to determine if the incoming stream has an embedded-signal therein;

an intervention component configured to intervene with clear reception of the subject incoming stream, thereby hindering detection by the detector, wherein the intervention component is further configured to modify the reception by introducing a countersignal into the incoming stream at the location in memory determined to be where the subject incoming stream is being received by the detector.

On pp. 6-7 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "memory-location determiner" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervention component" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determin[ing] where, in a memory, [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer has not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determin[ing] where, in a memory, [the detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "interven[ing] with clear reception of the subject input stream...hindering watermark detection by the detector...modify the reception by introducing a countersignal into the incoming stream at the location in memory determined to be where the subject incoming stream is being received by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. The "transformations" and "attacks", as listed and described by Cox, do not include "modify[ing] the reception by introducing a countersignal into the incoming stream at the location in memory determined to be where the subject incoming stream is being received by the detector." Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 51.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 51. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 51.

Independent Claim 52

Claim 52 recites, in part:

> determining where, in a memory, a dynamic watermark detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform watermark detection

thereon to determine if the subject input stream has an embedded-signal therein;

intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector; and

maintaining the intervening while the subject input stream is being played.

On p. 5 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "determining" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element. However, the Office fails to mention anything about the "maintaining" element of this claim.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determining where, in a memory, [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer has not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determining where, in a memory, [the detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (see Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "intervening with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks

such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Moreover, the Office fails to cite any reference as teaching "maintaining the intervening while the subject input stream is being played," as claimed. Both Lenoir and Cox are silent on this specific aspect of the claim.

Consequently, the combination of Lenoir and Cox does not teach or suggest at least this element of claim 52.

For at least the reasons presented herein, the combination of Lenoir and Cox does not teach or suggest all of the features of claim 52. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 52.

Claims 3, 11, 19, 46, 47, 53 and 54 are Non-Obvious Over Lenoir in View of Cox and Further in View of Tobias

Claims 3, 11, 19, 46, 47, 53 and 54 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Lenoir in view of Cox and further in view of Tobias. Applicant respectfully traverses the rejection.

Dependent Claims 3, 11 and 19

Claims 3, 11 and 19 ultimately depend from independent claims 1, 9 and 17, respectively. As discussed above, claims 1, 9 and 17 are allowable over the combination of Lenoir and Cox. Tobias is cited for its alleged teaching of the adjusting of the "play-rate" of the incoming stream. However, Tobias fails to remedy the deficiencies of Lenoir and Cox, as noted above with regard to independent claims 1, 9 and 17. Therefore, claims 3, 11 and 19 are also allowable over the cited documents of record for at least their dependency from allowable base claims, and also for the additional features that each recites.

Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claims 3, 11 and 19.

Independent Claim 46

Claim 46 recites, in part:

> determining where, in a processor-readable memory, a dynamic watermark detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform watermark detection thereon to determine if the subject input stream has a watermark therein;
>
> observing the watermark detector in the processor-readable memory of a computer to determine its location in such memory;
>
> intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the intervening comprises adjusting the "play-rate" of the input stream.

On pp. 8-9 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "determining" and the "observing" elements, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

In shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determining where, in a...memory, [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer has not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determining where, in a...memory, [the detector] receives a subject input stream."

Furthermore, Lenoir fails to teach "observing the watermark detector in the ...memory...to determine its location in such memory," as claimed. As noted above, Lenoir's watermark detector 4 is integrated with the block decoder 3. It is not part of the buffer 5, which Lenoir indicates might be vulnerable to hackers. (*See* col. 4, lines 11-13). The Office has not identified (with or without any particularity) where Lenoir, or any reference, teaches "observing the watermark detector in the ...memory...to determine its location in such memory," as claimed.

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed "interven[ing] with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks

such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Tobias is cited for its alleged teaching of the adjusting of the "play-rate" of the incoming stream. However, Tobias fails to remedy the deficiencies of Lenoir and Cox as noted above. Consequently, the combination of Lenoir, Cox and Tobias does not teach or suggest at least this element of claim 46.

For at least the reasons presented herein, the combination of Lenoir, Cox and Tobias does not teach or suggest all of the features of claim 46. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 46.

Independent Claim 47

Claim 47 recites, in part:

> observing a dynamic embedded-signal detection program module ("dynamic detector") in a processor-readable memory of a computer configured to dynamically detect watermarks in an input stream,
>
> based upon the observing, determining a location in the processor-readable memory, the location being where the dynamic detector receives a subject incoming stream for the dynamic detector to perform embedded-signal detection

thereon to determine if the subject incoming stream has an embedded-signal therein; and

intervening with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, wherein the intervening comprises adjusting "consumption-rate" of the incoming stream.

On pp. 9-10 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "observing" and "detecting" element and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

In shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir, col. 4, lines 1-18, the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (col. 4, lines 6-9).

This claim recites "determining a location in the...memory...where [the dynamic detector] receives a subject input stream." Lenoir "collects" and "stores" data in its

buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in Lenoir buffer is not been received by the Lenoir's watermark detector. Therefore, Lenoir fails to teach "determining a location in the...memory...where [the dynamic detector] receives a subject input stream."

Furthermore, Lenoir fails to teach "observing [the dynamic detector] in a...memory," and performing the determining "based upon the observing," as claimed. As noted above, Lenoir's watermark detector 4 is integrated with the block decoder 3. It is not part of the buffer 5, which Lenoir indicates might be vulnerable to hackers. (*See* col. 4, lines 11-13). The Office has not identified (with or without any particularity) where Lenoir or any reference teaches "observing [the dynamic detector] in a...memory," and performing the determining "based upon the observing," as claimed.

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes, "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes, "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (see Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed

"intervening with clear reception of the subject input stream...hindering watermark detection by the dynamic detector."

Cox describes a number of common signal transformations that a watermark should survive e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Tobias is cited for its alleged teaching of the adjusting of the "play-rate" of the incoming stream. However, Tobias fails to remedy the deficiencies of Lenoir and Cox, as noted above. Consequently, the combination of Lenoir, Cox and Tobias does not teach or suggest at least this element of claim 47.

For at least the reasons presented herein, the combination of Lenoir, Cox and Tobias does not teach or suggest all of the features of claim 47. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 47.

Independent Claim 53

Claim 53 recites, in part:

> determining a location in a processor-readable memory of a computer configured to dynamically detect an

embedded-signal in an input stream, the location being where a dynamic embedded-signal detection program module ("dynamic detector") receives a subject incoming stream for the dynamic detector to perform detection thereon to determine if the incoming stream has an embedded-signal therein;

intervening with clear reception of the subject incoming stream, thereby hindering detection by the dynamic detector; and

maintaining the intervening while the incoming stream is being presented.

On p. 5 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "determining" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervening" element. However, the Office fails to mention anything about the "maintaining" element of this claim. Also, this claim does not have the claim language (regarding adjusting the "play-rate") that the Office argues for its rejection based on Tobias.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

In shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector

operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "determining where, in a memory, [the detector] receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in the Lenoir buffer is not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "determining where, in a memory, [the detector] receives a subject input stream."

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed

"intervening with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Moreover, the Office fails to cite any reference as teaching "maintaining the intervening while the subject input stream is being played," as claimed. Both Lenoir and Cox are silent on this specific aspect of the claim.

Tobias is cited for its alleged teaching of the adjusting of the "consumption-rate" of the incoming stream. However, this claim does not have the claim language for which the Office relies upon in Tobias for its rejection. Regardless, Tobias fails to remedy the deficiencies of Lenoir and Cox, as noted above. Consequently, the combination of Lenoir, Cox and Tobias does not teach or suggest at least this element of claim 53.

For at least the reasons presented herein, the combination of Lenoir, Cox and Tobias does not teach or suggest all of the features of claim 53. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 53.

Independent Claim 54

Claim 54 recites, in part:

> a memory-location determiner ("watermark-detector detector") configured to detect and observe a dynamic watermark detection program module ("watermark detector") in the processor-readable memory of a computer to detect and determine the location of the watermark detector in such memory, the watermark-detector detector being further configured to detect and determine where, in the processor-readable memory, the watermark detector receives a subject input stream for the watermark detector to perform watermark detection thereon to determine if the subject input stream has a watermark therein;
>
> an intervention component configured to intervene with clear reception of the subject incoming stream by the watermark detector, thereby hindering detection by the watermark detector, the intervention component being further configured to intervene by one or more intervening actions, the intervening actions being selected from a group consisting of:
>
> adjusting play-rate of the incoming stream;
>
> adjusting "consumption-rate" of the incoming stream;
>
> introducing a countersignal into the incoming stream;
>
> introducing noise into the incoming stream; and

the intervention component being further configured to maintain intervention while the subject input stream is being consumed by the watermark detector.

On pp. 9-10 of the Action, the Office relies upon Lenoir (col. 1, lines 55-65; col. 4, lines 2-18) to teach all of the aspects of the claimed "memory-location determiner" element, and relies upon Cox (Abstract; sections 5 and 6) to teach all of the aspects of the claimed "intervention component" element. However, the Office fails to mention anything about the maintaining aspect of the intervention component.

Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of the subject input stream, Lenoir is focused on actions related to data that is already received and stored in a memory.

As shown in Fig. 1 of Lenoir (provided herein on p. 18) and described in Lenoir (col. 4, lines 1-18), the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenoir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing." (Col. 4, lines 6-9).

This claim recites "detect[ing] and determin[ing] where, in the...memory, the watermark detector receives a subject input stream." Lenoir "collects" and "stores" data in its buffer. According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive

data in order to process it. The data stored in the Lenoir buffer is not been received by the Lenoir watermark detector. Therefore, Lenoir fails to teach "detect[ing] and determin[ing] where, in the...memory, the watermark detector receives a subject input stream."

Furthermore, Lenoir fails to teach "detect[ing] and determin[ing] the location of the watermark detector memory," as claimed. As noted above, Lenoir's watermark detector 4 is integrated with the block decoder 3. It is not part of the buffer 5, which Lenoir indicates might be vulnerable to hackers. (*See* col. 4, lines 11-13). The Office has not identified (with or without any particularity) where Lenoir or any reference teaches "detect[ing] and determin[ing] the location of the watermark detector memory," as claimed.

Cox describes tampering with watermarks and to what extent a watermark can be resistant to tampering. Cox also describes a variety of possible attacks. (Cox, title and abstract). Cox describes "a number of common signal transformations that a watermark should survive, e.g., noise." (Cox, 5. Signal Transformation). Cox also describes "a series of attacks that can be mounted against an unrestricted-key watermark." (Cox, 6. Intentional Attack).

It appears the Office is relying upon Cox's teaching about different types of signal transformations and intentional attacks that might be made on a watermark (*see* Cox 6. Intentional Attack) with the specific language recited by the claim about intervening with watermark detection itself rather than attacking the watermark. Cox fails to list any attack or transformation of the watermark that teaches or suggests the claimed

"interven[ing] with clear reception of the subject input stream...hindering watermark detection by the detector."

Cox describes a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise." (Cox, 5 Signal Transformations). In section 6, Cox further describes intentional attacks such as exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. The "transformations" and "attacks", as listed and described by Cox, do not include any of the following intervening actions: "adjusting play-rate of the incoming stream; adjusting 'consumption-rate' of the incoming stream; introducing a countersignal into the incoming stream; introducing noise into the incoming stream." Instead, Cox describes pixel shifting, adding random noise of a similar amplitude, exploiting the watermark detector by accessing information about whether a content contains a watermark or not, attacking the watermark inserter, estimating the watermark and subtracting this from the marked image, and circumventing the copy control mechanism.

Tobias is cited for its alleged teaching of the adjusting of the "consumption-rate" of the incoming stream. However, this claim does not have the claim language for which the Office relies upon in Tobias for its rejection. Regardless, Tobias fails to remedy the deficiencies of Lenoir and Cox, as noted above.

Moreover, the Office fails to cite any reference as teaching "maintain[ing] the intervention while the subject input stream is being consumed by the watermark

detector," as claimed. Lenior, Cox and Tobias are silent on this specific aspect of the claim.

Consequently, the combination of Lenoir, Cox and Tobias does not teach or suggest at least this element of claim 54.

For at least the reasons presented herein, the combination of Lenoir, Cox and Tobias does not teach or suggest all of the features of claim 54. Accordingly, Applicant respectfully requests that the Office withdraw the 103 rejection of claim 54.

Conclusion

For at least the foregoing reasons, all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application.

If any issues remain that would prevent allowance of this application, Applicant requests that the Examiner contact the undersigned representative before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/kaseychristie40559/ Dated: 09/20/2010

Kasey C. Christie
(kasey@leehayes.com; 509-944-4732)
Registration No. 40,559